PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-059357

(43)Date of publication of application : 25.02.2000

(51)Int.Cl. H04L 9/32
G09C 1/00
H04L 9/08
H04L 12/28

(21)Application number : 10-224079

(22)Date of filing : 07.08.1998

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>

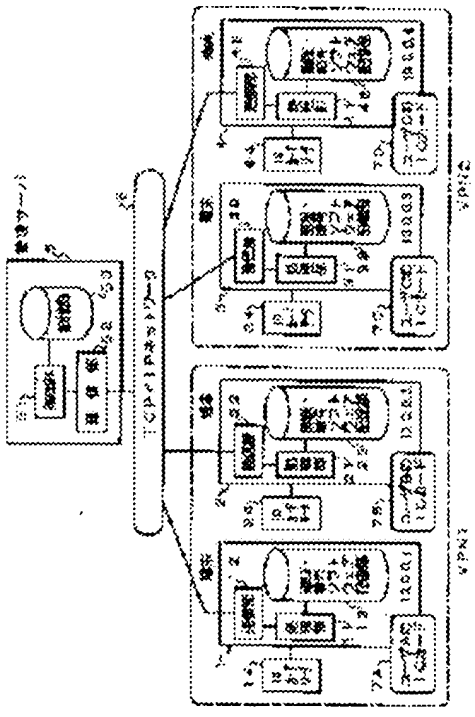
(72)Inventor : OKA KATSUYA
CHITOKU SHINYA
SAIJO TOMOYUKI
ONO HIROYASU

(54) CLOSED AREA GROUP COMMUNICATION SYSTEM, MANAGEMENT SERVER SYSTEM, COMMUNICATION TERMINAL AND THEIR PROGRAM STORAGE MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To build up a virtual private network VPN independently of a physical condition of a network such as a terminal utilizing IP address and a work place for the user in the case of building up the virtual private network VPN on the network using the TCP/IP.

SOLUTION: User Ids and passwords of all users using a network are registered by a management server 5 and an IC card 7 (A-D) is distributed to all the users. Furthermore, an authentication/encryption software and an IC card reader are provided to all terminals 1-4 on the network. The management server 5 configures a VPN in the unit of the user Ids and each user when using the network uses the IC card of the terminal and the user ID/password to receive the authentication by the management server 5. In this case, the management server 5 registers the IP address of the user terminal made to correspond to the VPN to which the user belongs so as to allow terminals used by users belonging to the same



VPN to configure the VPN.

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] The card mold storage which each user has, and the communication terminal which has the input/output interface of this card mold storage, A communication network is minded. It is the closed region group communication system which consists of management server equipment which distributes the cryptographic key for a communication link for performing a communication link within the closed region group between those communication terminals. Said card mold storage The information on the public key of said management server equipment and the private key of user each is held. Said management server equipment The means which carries out the management storage of the user ID belonging to the user ID and the password which were assigned to each user who uses said communication terminal beforehand, and two or more closed region group numbers and closed region groups, When the user ID and the password which have been transmitted from said communication terminal are decrypted using the private key of this management server equipment and user ID and a password are able to attest them The cryptographic key for a communication link of the closed region group to whom this user ID belongs is enciphered with the public key of a user with this user ID, and it has a means to transmit to said communication terminal. Said communication terminal The means which reads the public key of said management server equipment, and the private key of user each from said card mold storage inserted in said input/output interface, A means to encipher user ID and a password using the public key of this management server equipment, and to transmit to said management server equipment through a communication network, A means to receive the cryptographic key for a communication link with the communication terminal in a closed region group transmitted from said management server equipment, and to decrypt with the private key of said user each, Closed region group communication system characterized by having a means to encipher communication terminal mutual communication link information using the decrypted this cryptographic key for a communication link, and to perform the communication link between the communication terminals in a closed region group.
[Claim 2] As opposed to each user who distributes the cryptographic key for a communication link for performing a communication link within the closed region group between communication terminals through a communication network and who is management server equipment and performs a communication link within a closed region group beforehand The means which carries out the management storage of the user ID belonging to the user ID and the password which were assigned, and two or more closed region group numbers and closed region groups, The user ID and the password which were enciphered using the public key of this management server equipment read from the card mold storage with which it is the user ID and the password which have been sent from the communication terminal which said user uses, and this communication terminal was beforehand distributed to each user When it decrypts using the private key of this management server equipment and user ID and a password are able to be attested Management server equipment characterized by having a means to encipher the cryptographic key for a communication link of the closed region group to whom this user ID belongs with the public key of a user with this user ID, and to transmit to said

communication terminal.
[Claim 3] It is the communication terminal which communicates through a communication network using the cryptographic key for a communication link for performing a communication link within the closed region group between the communication terminals distributed from management server equipment. The input/output interface of a card mold storage, The means which reads the public key of said management server equipment, and the private key of user each from the card mold storage with which the information on the public key of said management server equipment and the private key of user each was stored beforehand through said input/output interface, A means to encipher user ID and a password using the public key of this management server equipment, and to transmit to said management server equipment through a communication network, A means to receive the cryptographic key for a communication link with the communication terminal in a closed region group transmitted from said management server equipment, and to decrypt with the private key of said user each, The communication terminal characterized by having a means to encipher communication terminal mutual communication link information using the decrypted this cryptographic key for a communication link, and to perform the communication link between the communication terminals in a closed region group.
[Claim 4] A communication network is minded. As opposed to each user who stored the program which the management server equipment which distributes the cryptographic key for a communication link for performing a communication link within the closed region group between communication terminals uses and who is a program storage and performs a communication link within a closed region group beforehand The processing which carries out the management storage of the user ID belonging to the user ID and the password which were assigned, and two or more closed region group numbers and closed region groups, The enciphered user ID which has been sent from said communication terminal, and the processing which decrypts a password using the private key of this management server equipment, The processing which attests the decrypted user ID and a password by collating with the user ID and the password which were registered beforehand, When user ID and a password are able to be attested, the cryptographic key for a communication link of the closed region group to whom this user ID belongs with the public key of a user with this user ID The program storage of the management server equipment characterized by storing the program which makes a calculating machine perform processing which is enciphered and is transmitted to said communication terminal.
[Claim 5] A communication network is minded using the cryptographic key for a communication link for performing a communication link within the closed region group between the communication terminals distributed from management server equipment. An input/output interface is minded from the card mold storage with which it is the program storage which stored the program which the communication terminal which communicates uses, and the information on the public key of said management server equipment and the private key of user each was stored beforehand. The processing which reads the public key of said management server equipment, and the private key of user each, The processing which enciphers user ID and a password using the public key of this management server equipment, and is transmitted to said management server equipment through a communication network, The processing which receives the cryptographic key for a communication link with the communication terminal in a closed region group transmitted from said management server equipment, and is decrypted with the private key of said user each, The program storage of the communication terminal characterized by storing the program which makes a computer perform processing which enciphers communication terminal mutual communication link information using the decrypted this cryptographic key for a communication link, and performs the communication link between the communication terminals in a closed region group.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] Using a TCP/IP protocol, this invention builds two or more imagination closed region groups (henceforth VPN) on the network where a terminal can communicate mutually, and relates to the closed region group communication system with which it was made for especially VPN not to depend on a user's work site only for the communication link between the users who belong at the same VPN with respect to the VPN construction technique of offering a possible environment, management server equipment, communication terminals, and those program storages.
[0002]
[Description of the Prior Art] When VPN was constituted from on a TCP/IP network, VPN was conventionally constituted by making into a unit the IP address which the terminal uses.
[0003] The 1st example of a system configuration of the former [drawing 10] and drawing 1111 show the 2nd conventional example of a system configuration. In drawing 10 and drawing 11 , the terminal 10 and the terminal 20 belong to same VPN1, and the terminal 30 and the terminal 40 belong to same VPN2. The management server 50 manages such VPN information. That is, the IP address assigned to each terminal fixed and the response relation between VPN1 and VPN2 are managed. The management server 50 and each terminal are connected through the TCP/IP network 60.
[0004] Although it is possible in drawing 10 for it to be recognized as User A and Users B being the terminals of the IP address in same VPN1 on the management server 50, and to communicate, if User B moves a work site like drawing 11 , since it will be recognized as it being in different VPN from the IP address of a terminal 10, and the IP address of a terminal 40 on the management server 50, User A cannot communicate with User B.
[0005]
[Problem(s) to be Solved by the Invention] When a user moves a work site to another terminal from the usually used terminal with the conventional technique, or when the usually used terminal is moved to another subnet and an IP address changes, it becomes the terminal and communication link impossible which belong to VPN which is different though the user was the same VPN. When such, it was required to make a setting-out change of the IP address of the terminal which constitutes VPN by the management server side which manages VPN one by one to communicate.
[0006] This invention aims at enabling a secure communication link among the users who belong to the same VPN, without making a setting-out change of an IP address, even when aiming at solution of the above-mentioned trouble and building VPN on a network, and the work site of the utilization IP address of a terminal or a user etc. enabled it to build VPN independent of network physical conditions, and a user changes a work site and uses other terminals.
[0007]
[Means for Solving the Problem] This invention is characterized [main] by enabling the configuration of VPN independent of a physical network by assigning all users unique user ID and a unique password within a system, changing the VPN configuration unit in a management server into user ID from the IP

address of the conventional terminal, and managing the translation table of the IP address of user ID and a terminal.
[0008] In case a user uses a communication network, user ID and a password are used and authentication by the management server is performed. The technique of VPN which made the conventional IP address the unit can be henceforth used as it is by registering into a management server the IP address of the terminal which a user uses at the time of authentication.
[0009] Moreover, safe authentication is enabled by using together the card mold storage (for example, IC card) other than user ID and a password to authentication.
[0010]
[Embodiment of the Invention] As a prerequisite of a [outline of gestalt of operation of this invention] book system, on the single closed region network which used the component of arbitration, the terminal shall belong to the subnet of arbitration and shall serve as an environment which can communicate mutually using a TCP/IP protocol. One accessible management server shall exist from all the terminals on a network, and authentication and code software, and IC card reader shall be installed in all the terminals linked to a network.
[0011] Under such a premise, the user ID and the password which become a meaning from an alphabetic character etc. to all network users (henceforth a user) are assigned, and it is set as a management server. On a management server, grouping of the user who can communicate mutually is carried out using user ID, and two or more imagination closed region groups (VPN) are created on a single network. In case a user uses a network, each terminal which the user who belongs to the same VPN uses constitutes VPN by inserting an IC card in IC card reader of a terminal, and performing authentication from a terminal using user ID and a password.
[0012] A secure communication link is attained among the users who belong to the same VPN, without being influenced by migration of a work station by building VPN using user ID.
[0013] [Utilization gestalt] drawing 1 shows the 1st example of a system configuration in the gestalt of operation of this invention. In this system, User A and User B belong to the same VPN, and User C and User D belong to the same VPN. The management server 5 memorizes and manages such VPN information in the storage section 53. The processing sections 51 are the part which performs processing of the management server 5, and a part into which the communications department 52 performs a communication link with each terminals 1-4 through the TCP/IP network 6.
[0014] Each terminals 1-4 have the authentication and the code software storage sections 13-43 which memorize the authentication and code software which the processing sections 11-41 which perform processing in a terminal, the communications departments 12-42 which communicate with the management server 5 or other terminals through the TCP/IP network 6, and the processing sections 11-41 perform. Moreover, each terminals 1-4 are equipped with the IC card readers 14-44 for reading IC cards 7A-7D which each user A-D has.
[0015] In drawing 1 , the terminal 3 and User D are working [User A / the terminal 1 and User B / the terminal 2 and User C] at the terminal 4. At this time, a terminal 1 and a terminal 2 can communicate and a terminal 3 and a terminal 4 can communicate. However, the communication link between the other terminals cannot be performed.
[0016] Drawing 2 shows the 2nd example of a system configuration in the gestalt of operation of this invention. In drawing 2 , the condition of the system of drawing 1 to the user A moves a work site to a terminal 3 from a terminal 1, and User C is moving the work site to the terminal 1 from the terminal 3. In this case, a terminal 1 and a terminal 3 can communicate and a terminal 2 and a terminal 4 can communicate. However, the communication link between a terminal 3 and a terminal 4 cannot be performed between a terminal 1 and a terminal 2.
[0017] Thus, since the terminal which constitutes VPN changes according to migration of a user, a communication link within VPN is possible for a user, without being dependent on a work site.
[0018] The work of each part in the system shown in [work of each part] drawing 1 and drawing 2 is as follows.
[0019] (a) Manage the response relation between the user ID of management server 5 and all network

users, a password, and Affiliation VPN.
- Manage the response relation between all network users' user ID, and each user's public key.
- Perform user authentication according to the demand from a terminal.
- If it succeeds in authentication, the IP address of the terminal which the user uses will be matched with user ID, and will be registered. The cryptographic key for a communication link required for each communication link in VPN is distributed to the terminal which the user uses.
[0020] (b) Authentication and the code software storage sections 13, 23, and 33, and 43 authentications and code software are built in all the terminals 1-4 linked to the TCP/IP network 6. User ID and a password are enciphered, it transmits to the management server 5, and authentication is received. Using the cryptographic key for a communication link distributed from the management server 5, a communication link packet is enciphered and a communication link mutual [between the terminals in VPN] is performed.
[0021] (c) Assign IC cards 7A-7D of one sheet for every IC card 7A-7D, IC card reader 14, 24, and 34, and 44 network user. The cryptographic key is stored in each of these IC cards, and a user can carry out transmission of user ID and a password, and reception of the cryptographic key for a communication link to insurance by using an IC card at the time of authentication.
[0022] [The description and an advantage]
- By using this system, VPN which made the user the unit can be constituted and the communication link security between the users in VPN is secured.
- Even if a user moves a work site, users' communication link and communication link security which belong to the same VPN are secured.
- By using an IC card, user authentication can be carried out to insurance.
[0023] [Flow of processing] drawing 3 is drawing explaining the actual example of the system shown in drawing 1 of operation. Drawing 4 is the processing flow chart of a terminal, and drawing 5 is the processing flow chart of a management server.
[0024] It precedes explaining actual actuation and a premise is explained briefly. Beforehand, a VPN utilization user shall access the management server 5, and shall register user ID, a password, and the VPN number to be used. Drawing 6 shows the example of the user ID which the VPN utilization user registered into the management server 5 beforehand, and a password.
[0025] The public key of the management server 5 and the private key for every user are stored in IC cards 7A-7D, respectively. For example, the public key of the management server 5 and User's A private key are stored in User's A IC card7A, and the public key of the management server 5 and User's B private key are stored in User's B IC card7B. Suppose that encryption and a decryption are performed with a public-key-encryption-ized method between a terminal and the management server 5. The private key of the management server 5 and the public key for every user are stored in the management server 5. Drawing 7 shows the example of the public key for every user which the management server 5 manages.

[0026] It is set up so that User A and User B may belong to VPN1 and User C and User D may belong to VPN2. The content of setting out is as being shown in drawing 6 . each user A-D -- User's A user ID -- USER-A and a password -- passwd1 -- the same -- User B -- USER-B and User C -- USER-C and User D -- USER-D -- as -- user ID is assigned, respectively.
[0027] In addition, the gestalt performed by the management server 5 is sufficient as issuance and management of IC cards 7A-7D, and issuance and management of the management server 5, and the public key and private key for every user, and the gestalt which receives and uses what an independent organization publishes is sufficient as them.
[0028] (1) hereafter shown in drawing 3 According to - (26), actuation of the system shown in drawing 1 R> 1 is explained.
(1) User A inserts IC card 7A in the IC card reader 14 of a terminal 1 to communicate with other users in the same VPN.
(2) Read the public key of the management server 5, and User's A private key from IC card7A to up to the memory of a terminal 1 by the IC card reader 14 (step S1 of drawing 4).

(3) A terminal 1 enters user ID and a password from User A (S2 of drawing 4).
(4) Encipher the user ID and the password which were entered with the public key of the management server 5 (S3 of drawing 4).
(5) A terminal 1 reads the IP address of the user ID enciphered to the management server 5, a password, and a terminal 1, and transmit it (S4 of drawing 4).
(6) The management server 5 decrypts user ID and a password for the authentication packet (the user ID and the password which were enciphered) from a terminal 1 with the private key of reception (S21 of drawing 5), and the management server 5 (S22 of drawing 5).
(7) Next, the management server 5 attests as compared with the content of registration which shows user ID and a password to drawing 6 (S23 of drawing 5).
(8) If it succeeds in this authentication, the management server 5 investigates VPN to which User A belongs, will match with VPN1 source IP address 10.0.0.1 in the authentication packet sent by User A, and will register it into the IP address column of the table shown in drawing 6 R> 6 (S24 of drawing 5). In addition, when automatic setting of the IP address is not carried out by communicating software into the authentication packet which transmits to the management server 5 from a terminal 1, the form which reads the IP address of a terminal 1 and is transmitted to the management server 5 is sufficient.
(9) The management server 5 enciphers the cryptographic key for a communication link required in order that a terminal 1 may communicate within VPN1 with User's A public key (S25 of drawing 5). Under the present circumstances, the data of the public key managed table (drawing 7) for every user ID registered beforehand are used.
(10) The management server 5 transmits the cryptographic key for a communication link of enciphered VPN1 to a terminal 1 (S26 of drawing 5).
(11) Terminal 1 The cryptographic key for a communication link of enciphered VPN1 is received from the management server 5 (S5 of drawing 4), and it decrypts with User's A private key (S6 of drawing 4).
(12) A terminal 1 returns the reception response of the cryptographic key for a communication link to the management server 5 (S7 of drawing 4).
(13) - (24) At a terminal 2, when User B inserts IC card 7B in the IC card reader 24, authentication processing to User B is performed similarly, and the cryptographic key for a communication link of VPN1 is distributed to a terminal 2.
(25) - (26) Since a terminal 1 and a terminal 2 constitute VPN1 with the same cryptographic key for a communication link by the above processing, the data encryption which used the cryptographic key for a communication link of VPN1 performs the communication link between a terminal 1 and a terminal 2 henceforth (S9 of drawing 4). In addition, the IP address of the users which perform the communication link in VPN can perform the communication link between a terminal 1 and a terminal 2 by accessing the management server 5 and receiving.
[0029] VPN2 is constituted by performing same processing also about User C and User D. The configuration information to which the management server 5 after a carrier beam manages [User A, User B, User C, and User D] authentication, respectively changes like drawing 8 .
[0030] It becomes the following actuation in changing from the condition of the system configuration shown in drawing 1 to the condition of the system configuration shown in drawing 2 . Drawing 9 is drawing explaining actuation in case User A and User C stop an activity with a terminal 1 and a terminal 3. (1) hereafter shown in drawing 9 The actuation is explained according to - (12).
(1) User A samples IC card 7A from the IC card reader 14 of a terminal 1. A terminal 1 detects sampling of this IC card 7A (S11 of drawing 4).
(2) Thereby, the deletion demand of the public key the management server's 5 and User's A private key stored on memory occurs to a terminal 1.
(3) A terminal 1 deletes the public key of the management server 5, and User's A private key from on memory (S12 of drawing 4).
(4) A terminal 1 transmits an IP address clear demand of User A to the management server 5 (S13 of drawing 4).

(5) The management server 5 receives an IP address clear demand of the user A from a terminal 1 (S31 of drawing 5), and clears User's A IP address (S32 of drawing 5).
(6) The management server 5 returns an IP address clear response to a terminal 1 (S33 of drawing 5).
(7) - (12) Processing with the same said of User C is performed.
[0031] It will be in the condition before, as for a terminal 1 and a terminal 3, User A and User C receive authentication by the above no longer the configuration member of return and VPN. Then, User A receives authentication at a terminal 3, and User C receives authentication at a terminal 1. At this time, a terminal 2 and a terminal 3 constitute VPN1, and a terminal 1 and a terminal 4 constitute VPN2. By this, the communication link of User A, User B, User C, and User D is attained within each VPN.
[0032] In addition, although the above explanation explained the example which used the IC card as a card mold storage, if it is a storage, even if it is the storage of a magnetic card, a magneto-optic-recording card, and,others, it can carry out. moreover, the thing of the pocket mold with which the terminal did not need to be fixed and card mold storage reader/writer was built in -- you may be -- a communication network -- a cable/wireless -- this invention can be carried out with any gestalt.
[0033] A program for each computer of the management server 5 and terminals 1-4 to realize each above processing is storable in suitable storages, such as portable medium memory which a computer can read, semiconductor memory, and a hard disk.
[0034]
[Effect of the Invention] As explained above, according to this invention, VPN which does not depend for a user on the IP address made into the unit can be constituted. Therefore, the communication link from which communication link security was secured among the users who are not dependent on a work site and belong to the same VPN is possible for a user.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is drawing showing the 1st example of a system configuration in the gestalt of operation of this invention.
[Drawing 2] It is drawing showing the 2nd example of a system configuration in the gestalt of operation of this invention.
[Drawing 3] It is drawing explaining the actual example of the system shown in drawing 1 of operation.
[Drawing 4] It is the processing flow chart of a terminal.
[Drawing 5] It is the processing flow chart of a management server.
[Drawing 6] It is drawing showing the example of the user ID which the VPN utilization user registered into the management server, and a password.
[Drawing 7] It is drawing showing the example of the public key for every user which a management server manages.
[Drawing 8] It is drawing showing the example of the VPN configuration information which a management server manages.
[Drawing 9] It is an explanatory view of operation in case a user stops an activity with a terminal.
[Drawing 10] It is drawing showing the 1st conventional example of a system configuration.
[Drawing 11] It is drawing showing the 2nd conventional example of a system configuration.
[Description of Notations]
1, 2, 3, 4 Terminal
11, 21, 31, 41 Processing section
12, 22, 32, 42 Communications department
13, 23, 33, 43 Authentication and the code software storage section
14, 24, 34, 44 IC card reader
5 Management Server
51 Processing Section
52 Communications Department
53 Storage Section
6 TCP/IP Network
7A, 7B, 7C, 7D IC card

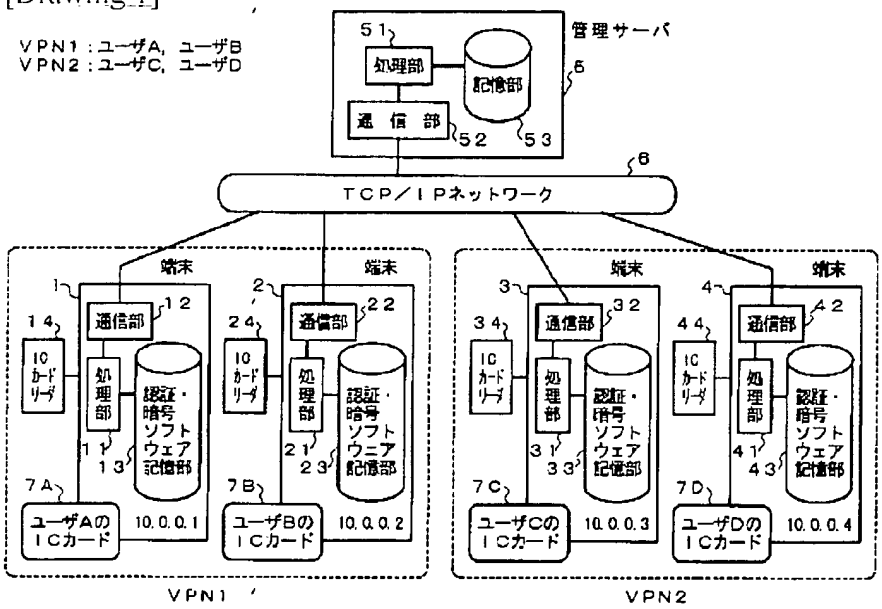
[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

[Drawing 1]



[Drawing 6]

VPN1

ユーザID	パスワード	IPアドレス
USER-A	passwd1	-
USER-B	passwd2	-

VPN2

ユーザID	パスワード	IPアドレス
USER-C	passwd3	-
USER-D	passwd4	-

[Drawing 7]

ユーザID	公開鍵
USER-A	56978
USER-B	ab379
USER-C	xy115
⋮	⋮

[Drawing 8]

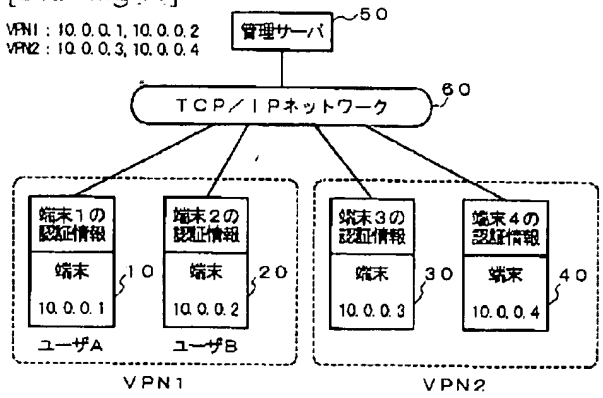
VPN1

ユーザID	パスワード	IPアドレス
USER-A	passwd1	10.0.0.1
USER-B	passwd2	10.0.0.2

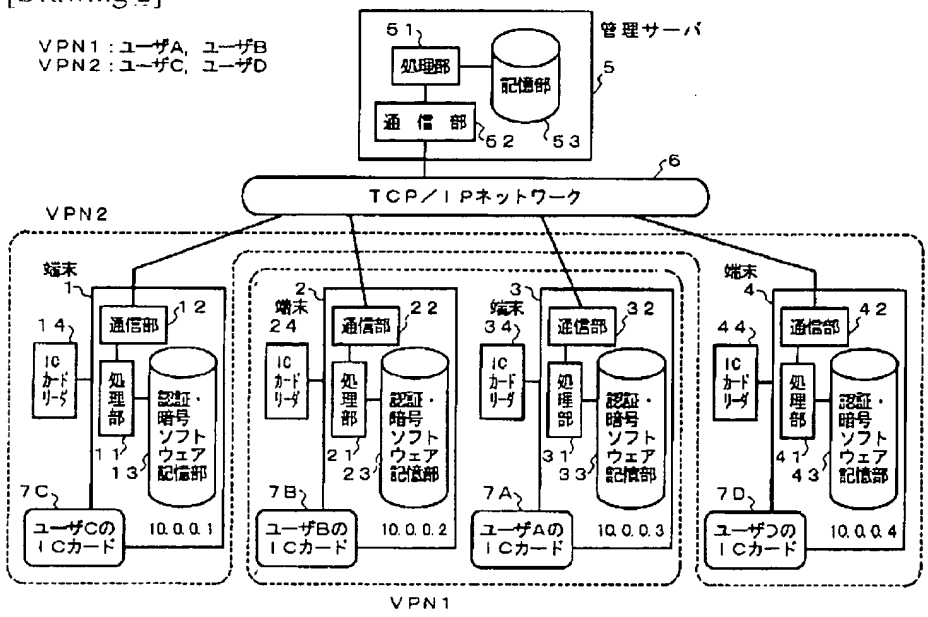
VPN2

ユーザID	パスワード	IPアドレス
USER-C	passwd3	10.0.0.3
USER-D	passwd4	10.0.0.4

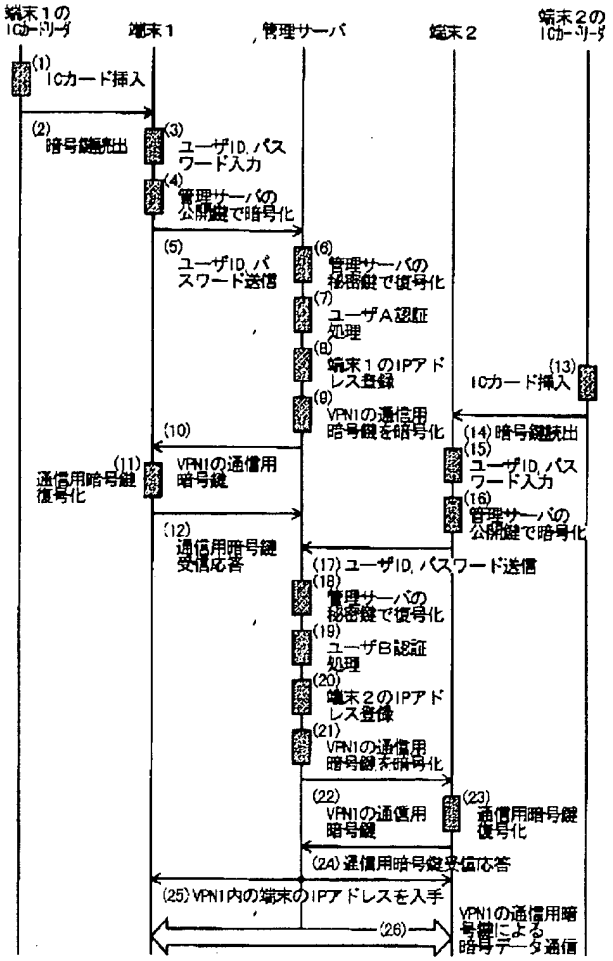
[Drawing 10]



[Drawing 2]

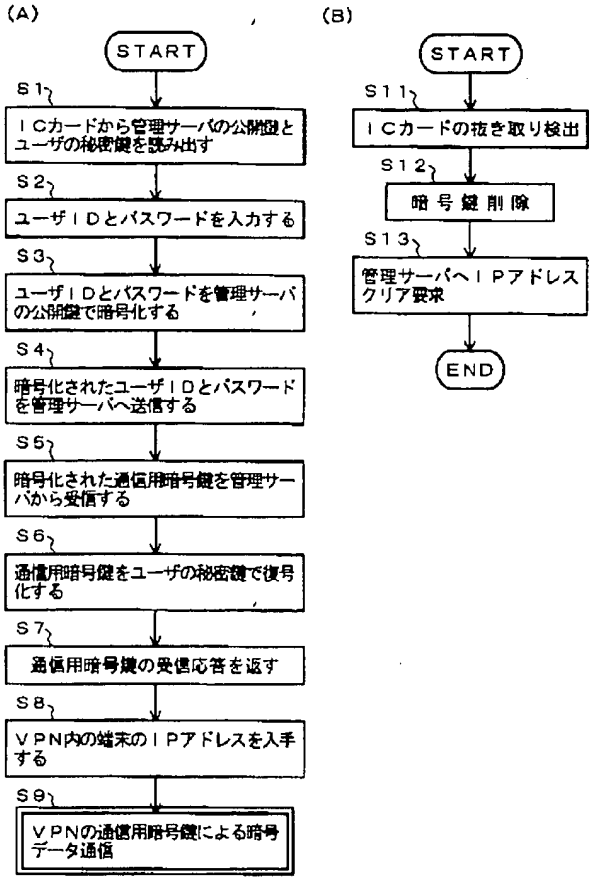


[Drawing 3]


端末1の ICカードリーダ
端末1
管理サーバ
端末2
端末2の ICカードリーダ
(1) ICカード挿入
(2) 暗号鍵読出
(3) ユーザID,パスワード入力
(4) 管理サーバの公開鍵で暗号化
(5) ユーザID,パスワード送信
(6) 管理サーバの秘密鍵で復号化
(7) ユーザA認証処理
(8) 端末1のIPアドレス登録
(9) VPN1の通信用暗号鍵を暗号化
(10)
(11) VPN1の通信用暗号鍵 通信用暗号鍵復号化
(12) 通信用暗号鍵受信応答
(13) ICカード挿入
(14) 暗号鍵読出
(15) ユーザID,パスワード入力
(16) 管理サーバの公開鍵で暗号化
(17) ユーザID,パスワード送信
(18) 管理サーバの秘密鍵で復号化
(19) ユーザB認証処理
(20) 端末2のIPアドレス登録
(21) VPN1の通信用暗号鍵を暗号化
(22) VPN1の通信用暗号鍵
(23) 通信用暗号鍵復号化
(24) 通信用暗号鍵受信応答
(25) VPN1内の端末のIPアドレスを入手
(26)
VPN1の通信用暗号鍵による暗号データ通信

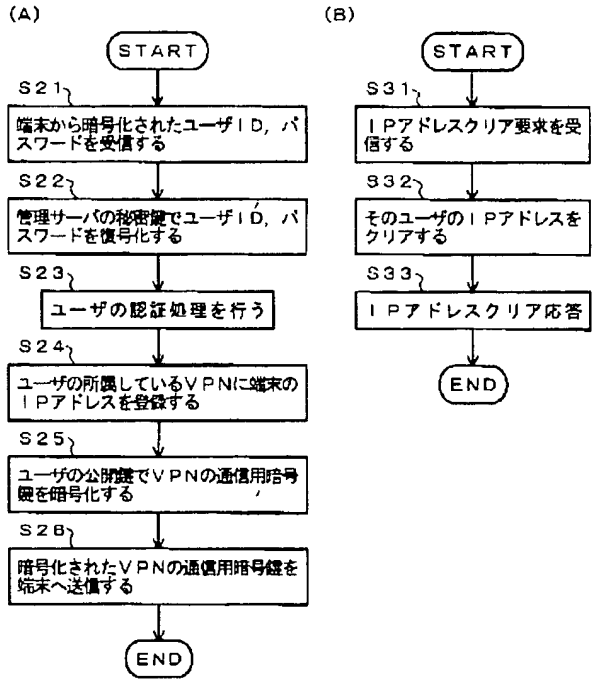
[Drawing 4]

端末の処理フローチャート

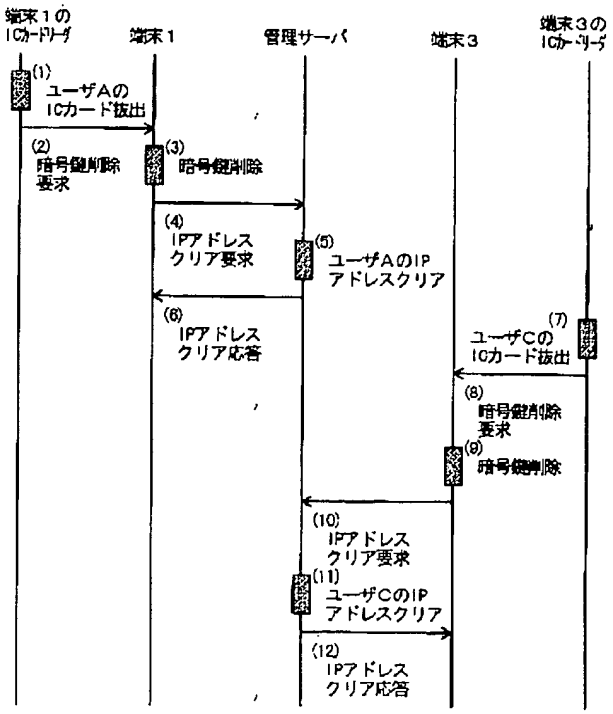


[Drawing 5]

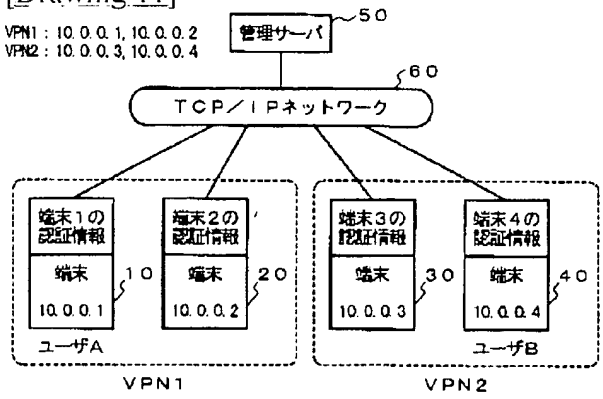
管理サーバの処理フローチャート



[Drawing 9]



[Drawing 11]



[Translation done.]